UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched

903 Frank Wicker Road, Sanford, North Carolina

Case No. 1:18mj317

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment C

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC 841/846	Conspiracy to Distribute Controlled Substances
21 USC 843(b)	Use of a Comm. Facility to Commit Controlled Substance Offense

The application is based on these facts:

See Attachment A

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DEA Special Agent Stephen Razik
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/22/18

Judge's signature

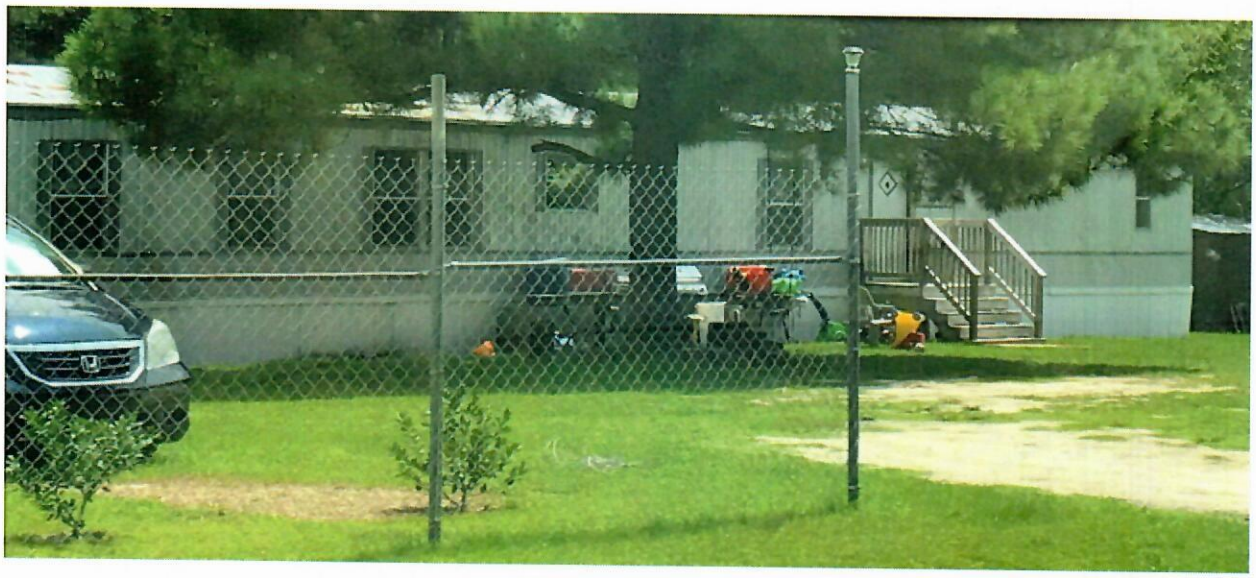
City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge
Printed name and title

ATTACHMENT C

Description of Search Location

903 Frank Wicker Road, Sanford, North Carolina is a single-wide trailer dwelling constructed primarily of metal material, light colored siding with white and blue colored trim. The top portion of the trailer is silver in color and the bottom section is white. There is a wooden front porch leading up to the front door. The front door is white in color with a diamond shape ornamental marking on the top portion of the door. There is a chain link fence surrounding the perimeter of the property, with an opening on the Frank Wicker Road side for passage of vehicles. There is a large tree in the front yard of the property. Additionally, 903 Frank Wicker Road, Sanford, North Carolina has a front door facing the roadway of Frank Wicker Road and the numbers "903" appear in black color to the right side of the door on the trailer, indicating 903 as the address of the residence. (See photo below)



ATTACHMENT B
Items to be Seized

The following items which constitute fruit, instrumentalities, or evidence of violations of:

a. Possession with intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841, and conspiracy to commit this offense, in violation of Title 21, United States Code, Section 846; and,

b. Use of a communication facility in committing controlled substances offenses, in violation of Title 21, United States Code, Sections 843(b);

1. Controlled substances, specifically including, but not limited to: a) cocaine; b) other illicit controlled substances; and c) residue of each particular illicit drug.

2. Items used in the sale, transfer, transportation, packaging and use of cocaine, including, but not limited to; scales, packaging materials, plastic wrap, plastic bags, written articles on the use and effects of narcotics, diluents and cutting agents.

3. Documents revealing, referencing, and/or memorializing the ordering, purchasing, storage, transportation and sale of controlled substances, including, buyer lists, seller lists, pay-owe sheets and records of sales, log books, drug ledgers, personal telephone/address books of customers and suppliers, rolodexes, telephone answering pads, bank and financial records, records relating to domestic and foreign travel such as tickets, passports, visas, credit card receipts, travel schedules, receipts and records, trucker log books and storage records, such as storage locker receipts and safety deposit box rental records.

4. Proceeds and articles of personal property which are the fruits, instrumentalities and evidence of trafficking in controlled substances, including U.S. currency, precious metals and stones, jewelry, negotiable instruments and financial instruments including stocks and bonds.

5. Photographs of participants and fruits and evidence of the trafficking of controlled substances.

6. Documents and articles of personal property showing or containing data showing the identity of persons occupying, possessing, residing in, owing, frequenting or controlling the premises to be searched or property therein, including keys, rental agreements and records, property acquisition records, utility and telephone bills and receipts, photographs, cellular telephones, wireless telephones, rolodexes, telephone answering pads, storage records, vehicle or vessel records, canceled mail envelopes, correspondence, opened or unopened, financial documents such as tax returns, bank records, safety deposit box

records, canceled checks and other records of incomes and expenditures, credit card and bank records.

7. Weapons, including firearms and ammunition.

8. Waybills, air bills, bills of lading, receipts, delivery notices, and other shipping documentation from the U.S. Postal Service, small package carriers, or common carriers which indicate the shipment of packages and parcels.

As used above, the terms records, documents, messages, correspondence, data, and materials includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored.

For any digital device or storage medium whose seizure is authorized by this warrant, and any digital device or storage medium that contains or in which is stored records or information that is otherwise contemplated by this warrant (hereinafter, "device"):

1. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;

2. Evidence of software — or absence thereof — that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the attachment to the device of other storage devices or similar containers for electronic evidence;

4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

5. Passwords, encryption keys, and other means to access the device;

6. Documentation and manuals that may be necessary to access the device or conduct a forensic examination of the device;

7. Records of or information about Internet Protocol addresses used by the device;

8. Records of or information about the device's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses revealing the possession or trafficking of controlled substances;

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); and handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "device" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, smart phones, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, such as hard drives, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT A

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Stephen Razik, a Special Agent with the Drug Enforcement Administration (DEA), being duly sworn, state as follows:

INTRODUCTION

1. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am a Special Agent of the Drug Enforcement Administration (DEA). I have been employed by the DEA since June 1997 and am currently assigned to the DEA Greensboro Resident Office (GRO). I have attended numerous training programs relating to drug trafficking, and I am experienced in investigating drug traffickers. I am familiar with the use of various forms of electronic surveillance as investigative tools. I have participated in investigations involving cocaine hydrochloride (HCl), cocaine base (crack), marijuana, methamphetamine, heroin, and various other controlled substances. For approximately five years, prior to working for DEA, I was a Florida State Trooper stationed in Miami, Florida. As a DEA Special Agent, I have participated in investigations involving, but not limited to, physical surveillance, undercover transactions, court ordered pen registers, the use of wire and electronic communication interceptions, and both state and federal search warrants. I have received training, both formal and informal, in the investigation of drug trafficking and money laundering, including, but not limited to, DEA basic

and advanced drug investigations courses; street level drug enforcement; narcotics interdiction; wiretap investigations; and the DEA Basic Agent Training Academy located at Quantico, Virginia.

2. Through my training, education and work experience, I have become familiar with the manner in which drug trafficking violations are committed. Based on my training and experience and participation in controlled substance investigations, which result from violations of narcotics laws, I know:

a. That drug traffickers maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers relating to the importation, transportation, ordering, sale, purchase, and distribution of controlled substances and firearms.

b. That these aforementioned books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers are readily available to the drug traffickers such as in their residences, places of business, and alternate storage locations (such as mini-storage facilities).

c. That it is common for drug traffickers to secrete contraband, including but not limited to packaging material and other paraphernalia, in secure locations for ready access, and to conceal them from law enforcement.

d. That persons involved in drug trafficking conceal in secure locations, with ease of access, large amounts of currency and other proceeds of drug and firearm transactions, and financial instruments and other evidence of financial transactions relating to the obtaining, transfer, secreting, and spending of drug and/or firearm transaction proceeds.

e. That drug traffickers commonly maintain addresses or telephone numbers, in books or papers, which reflect names, addresses, and/or telephone numbers for associations in the

drug trafficking organization, and keep these records in their residences, places of business and mini-storage facilities, vehicles, safes and/or locked boxes, vehicles, storage buildings and/or sheds on the property.

f. That firearms are considered "tools of the drug trafficking trade." That is, traffickers often possess firearms to protect themselves, their drugs, their firearms, and their proceeds from law enforcement, competitor drug traffickers, and would-be thieves.

g. That the drug traffickers take or cause to be taken photographs of them, their associates, their property and their drugs, and that they usually keep these photographs in their residences, places of business, vehicles, safes and/or locked boxes, storage buildings and/or sheds on the property and alternative storage locations with other drug-related documents.

h. That drug traffickers commonly use electronic devices, such as cellular telephones, computers, and other personal electronic devices to facilitate the purchase and sale of narcotics. Drug traffickers utilize cellular telephone devices to coordinate drug transactions, store information concerning their customers, and take photographs of their supply.

4. This affidavit contains information necessary to support probable cause for a Search Warrant for the premises located at 903 Frank Wicker Road, Sanford, North Carolina (the **Target Location**), for evidence related to violations of Title 21, United States Code, Sections 841(a)(1), 843(b), and 846. This affidavit also contains information necessary to support probable cause for a Search Warrant for a gray Dodge Ram pick-up truck bearing North Carolina plate HT 2695, VIN 1D7HU18D74J265329 (the **Target Vehicle**), for evidence related to violations of Title 21, United States Code, Sections 841(a)(1), 843(b), and 846. Each premise to be searched is described further

in the Attachment C appended to the corresponding search warrant application. Likewise, the things to be searched for and seized are further described in the Attachment B appended to the corresponding search warrant application.

5. The information contained in this Affidavit is based on my personal participation in the investigation of this case and from information provided to me by other Special Agents and Task Force Officers, as well as other federal, state, and local law enforcement agents and officers. Since this Affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a Search Warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts which I believe are necessary to establish the requisite foundation for probable cause.

6. In this case, law enforcement is planning the coordinated arrest of multiple defendants, to be carried out at the same time as multiple search warrants in three different federal districts. I know that, ordinarily, search warrants are authorized for execution between the hours of 6:00 a.m. and 10:00 p.m.; however, I am seeking authorization to execute the search warrants outside of these hours. This is necessary because, in this case, some of the defendants work in construction, and therefore typically leave for work well before 6:00 a.m. Thus, in order to effect simultaneous arrests of all defendants — thereby avoiding the possibility that any defendant would be tipped off to the investigation and evade prosecution and/or destroy evidence — the arrest warrants will be executed outside the window of 6:00 a.m. to 10:00 p.m. Therefore, good cause exists to execute the search warrants outside of this window as well.

FACTS ESTABLISHING PROBABLE CAUSE

7. In and around December 2017, based on information from a confidential source (CS), the FBI began to investigate the drug trafficking activity of Reyes BARRERA ALACHAN. The CS introduced an undercover law enforcement officer (UC-1) to BARRERA ALACHAN, and following that initial introduction, law enforcement has conducted several controlled purchases of distribution quantities of powder cocaine (to date, totaling approximately 26 and a quarter ounces, or approximately 735 grams), as well as several firearms, as set forth below.

8. The CS will be referred to herein using masculine pronouns regardless of actual gender. The CS has a criminal history and has been convicted of charges related to gang involvement, destruction of property, distribution of marijuana, and DWI. He has also been charged with offenses related to firearms, drug possession, grand larceny, and failure to appear, which were resolved via nolle prosequi.

9. The CS has been working with law enforcement since in and around June 2015. The CS has provided reliable information to law enforcement on multiple occasions, including information that has resulted in criminal convictions of other individuals. In exchange for the CS's cooperation, the CS has received reduced sentences for the offenses listed above. The CS has not received financial compensation for his cooperation.

10. The CS's information regarding BARRERA ALACHAN has been corroborated through controlled purchases of cocaine and firearms from BARRERA ALACHAN using undercover officers, as well as through toll records and physical and electronic surveillance, as set forth below.

11. In addition to the use of the CS and undercover officers, surveillance, and other traditional investigative techniques, law enforcement also utilized the authorized interception of wire and electronic communications over two cellular phones used by BARRERA ALACHAN and co-conspirator Homero SALGADO Alvarez, respectively. On May 24, 2018, the Honorable Claude M. Hilton, United States District Judge for the Eastern District of Virginia, authorized the initial interception of wire and electronic communications occurring to and from BARRERA ALACHAN's cell phone (TARGET TELEPHONE 1, or "TT1"). On June 26, 2018, Judge Hilton extended the interception of wire and electronic communications to and from TT1, and authorized the initial interception of wire communications to and from SALGADO's cell phone (TARGET TELEPHONE 2, or "TT2"). On or about July 19, 2018, law enforcement ceased interception of TT1. On July 25, 2018, Judge Hilton extended the interception of wire communications, and authorized the initial interception of electronic communications, to and from TT2.

12. Dozens of intercepted communications have been pertinent to this investigation. Any statements excerpted from recorded conversations, including those that are quoted, are subject to further revision for clarification and/or accuracy. Quoted segments from intercepted communications are based on line sheets and reviews of recordings, and are not final or certified transcripts. In addition, all dates and times are approximate and based on the monitoring equipment at the time the communication was intercepted. Not all relevant intercepted communications are described, and not all relevant portions of mentioned communications have been described. Among other things, brackets are used to provide certain contextual information, such as when the intercepted communications were unintelligible, or when the transcript is based

on a phonetic interpretation of the intercepted communication.

13. On or about January 15, 2018, law enforcement obtained a search warrant for real-time GPS location data on TT1. On or about January 19, 2018, GPS location data showed that BARRERA ALACHAN traveled to Sanford, North Carolina, where he stayed for the night in the area of the **Target Location**, a residence associated with co-conspirator Homero SALGADO Alvarez. A review of toll records for BARRERA ALACHAN showed that while traveling to North Carolina, BARRERA ALACHAN called TT2, which lists the **Target Location** as the subscriber address. Law enforcement subsequently determined through physical and electronic surveillance that SALGADO uses TT2.

14. The next day, on or about January 20, 2018, BARRERA ALACHAN communicated with UC-1 via TT1 to arrange a deal to sell UC-1 three ounces of cocaine. Most, if not all, of the calls and text messages were recorded. BARRERA ALACHAN agreed to meet UC-1 in an undercover vehicle in a parking lot in Prince William County, that day. Prior to the meeting, BARRERA ALACHAN called UC-1 and said "you right here?" UC-1 responded "yes, I was at the light." Later in the conversation, UC-1 asked BARRERA ALACHAN, "are you there?" BARRERA ALACHAN answered "Yes, I'm…here- - here." At the meeting, UC-1, who was wearing an audio recording device, gave BARRERA ALACHAN $2,700 of controlled funds and received three ounces of suspected cocaine. The substance later field-tested positive for the presence of cocaine.

15. Following the deal, surveillance continued to monitor BARRERA ALACHAN as he left and traveled back up to Maryland. At approximately 1:39 p.m., surveillance observed

BARRERA ALACHAN arrive at his residence in Catonsville, Maryland. At approximately 4:15 p.m., GPS location data on TT1 showed it begin to move south again, to the area of the **Target Location**. Shortly after TT1 arrived at the **Target Location**, it began moving back north and then returned to Catonsville. Based on my training, experience, and knowledge of this case, I believe that the purpose of the two trips BARRERA ALACHAN took to the **Target Location** on January 19 and 20 was to be resupplied with cocaine by SALGADO, suspected to be his supplier.

16. On or about January 27, 2018, GPS location data showed that BARRERA ALACHAN traveled from Maryland to North Carolina again. BARRERA ALACHAN stopped in Fayetteville, North Carolina, for approximately thirty minutes before returning to the Washington, DC area. On his return trip, BARRERA ALACHAN communicated with UC-1 via TT1 to arrange a deal to sell UC-1 a quantity of cocaine. Most, if not all, of the calls and text messages were recorded. Prior to the deal, UC-1 called BARRERA ALACHAN asking how long before he arrived at the site. While discussing the pending transaction, BARRERA ALACHAN told UC-1 that he had "*only two*" ounces of cocaine to sell him because someone else "*stole*" his "*business*." BARRERA ALACHAN agreed to meet UC-1 in an undercover vehicle in the same meeting location in Prince William County that day. At the meeting, UC-1 gave BARRERA ALACHAN $1,800 of controlled funds and received two ounces of suspected cocaine. The substance later field-tested positive for the presence of cocaine.

17. On or about February 5, 2018, GPS location data showed that BARRERA ALACHAN again traveled from Maryland to Fayetteville, North Carolina. While traveling to North Carolina, BARRERA ALACHAN communicated with the CS via phone calls and text messages on TT1 to

set up a cocaine sale on that same day. Most, if not all, of the calls and texts were recorded. According to GPS data, on this trip, BARRERA ALACHAN stayed in Fayetteville for approximately thirty minutes before returning to the Washington, DC area. UC-1 sent a text message to BARRERA ALACHAN on TT1 and asked in Spanish "you have 4?" BARRERA ALACHAN texted back "3." It is my understanding through my training, experience, and knowledge of this investigation, that UC-1 asked BARRERA ALACHAN if he had four ounces of cocaine to sell to UC-1, and that BARRERA ALACHAN responded that he only had three ounces to sell. BARRERA ALACHAN met with UC-1 and another undercover officer ("UC-2") in a parking lot in Prince William County, Virginia. The undercover vehicle was equipped with audio and video recording devices. The video equipment malfunctioned, but the audio still recorded. BARRERA ALACHAN got into the undercover vehicle and exchanged three ounces of suspected cocaine for $2,700 dollars in controlled funds. The substance later field-tested positive for the presence of cocaine.

18. On or about February 13, 2018, UC-1 communicated with BARRERA ALACHAN on TT1 to purchase a quantity of powder cocaine. BARRERA ALACHAN stated, "I have… eh, two cans of paint and a *seven, seven*." UC-1 responded "a seven of what?" BARRERA ALACHAN again said "I have a seven, seven or two two twenty five. You want the seven as well?" Based on my training, experience, and knowledge of this investigation, I believe that by "two cans of paint," BARRERA ALACHAN was using code to refer to two ounces of cocaine. I further believe that by "and a seven" or "two twenty five," BARRERA ALACHAN meant that he had an additional seven grams (one-quarter ounce) of cocaine available, for a total of 2.25 ounces. UC-1 and

BARRERA ALACHAN negotiated a price of $200 for the seven grams, and UC-1 agreed to purchase the two ounces as well. BARRERA ALACHAN met with UC-1 and UC-2 at a parking lot in Prince William County, Virginia. UC-1 exchanged $2,000 in controlled funds for approximately 62 grams (approximately 2.25 ounces) of powder cocaine. The transaction was only audio recorded. The cocaine was field tested and returned positive for the presence of cocaine.

19. On or about February 22, 2018, UC-1 communicated with BARRERA ALACHAN via TT1 to arrange a purchase of cocaine. UC-1 texted BARRERA ALACHAN, "*What's up bro*" and "You have the three cans of paint for today?" BARRERA ALACHAN responded, "yes." Based on my training, experience, and knowledge of this investigation, I believe that when UC-1 asked about the "three cans of paint," BARRERA ALACHAN understood him to be referring to three ounces of cocaine. Thereafter, UC-1 and UC-2 traveled to Ellicott City, Maryland, and met BARRERA ALACHAN and an individual subsequently identified as Danior BARRERA REINA in a parking lot, where UC-1 purchased three ounces of powder cocaine from BARRERA ALACHAN in exchange for $2,700 in controlled funds. The cocaine was field tested and returned positive for the presence of cocaine.

20. The February 22 transaction was completed at approximately 5:18 p.m. Approximately an hour and a half later, BARRERA ALACHAN called SALGADO on TT2.

21. On or about February 24, 2018, GPS location data for TT1 showed that BARRERA ALACHAN traveled from Maryland to North Carolina. At approximately 7:35 p.m., TT1 arrived in the vicinity of the **Target Location**. Between the hours of 7:35 p.m. and 6:38 a.m. on February

25, 2018, GPS pings placed TT1 at the **Target Location**, with uncertainty ranges of between nine and twenty-five meters. At approximately 6:54 a.m., GPS location data showed that TT1 started to travel north back to the Washington, DC area.

22. On or about March 14, 2018, UC-1 communicated with BARRERA ALACHAN via TT1 regarding purchasing a quantity of cocaine. UC-1 called BARRERA ALACHAN and asked, "Can you do 4?," to which BARRERA ALACHAN responded, "Yes." This call was recorded. Based on my training, experience, and knowledge of this case, I believe that the UC-1 asked BARRERA ALACHAN if he could sell UC-1 four ounces of cocaine. Shortly after speaking with UC-1, BARRERA ALACHAN, using TT1, called SALGADO on TT2.

23. On or about March 16, 2018, at approximately 2:16 p.m., law enforcement surveillance observed BARRERA ALACHAN's vehicle parked in the vicinity of his residence at 318 Melvin Avenue in Catonsville, Maryland.

24. Shortly thereafter, GPS location data for TT1 showed that BARRERA ALACHAN traveled from Maryland to Sanford, North Carolina. Law enforcement surveillance in Sanford observed a dark-colored compact sedan parked at the **Target Location**, the residence associated with SALGADO. A GPS ping at approximately 9:53 p.m. revealed that TT1 was located at the **Target Location**, with an uncertainty range of approximately nine meters in diameter.

25. Approximately fifteen minutes later, the next GPS ping showed that TT1 was approximately twelve miles north of the **Target Location**, within an uncertainty range of approximately fourteen meters. Around the same time, law enforcement drove by the **Target Location** and observed that the dark-colored compact sedan was no longer parked at the house.

26. At approximately 10:42 p.m., law enforcement observed what appeared to be the same dark-colored compact sedan, occupied by two individuals, near the I-40 interchange with Route 1, between Cary and Raleigh, North Carolina. Law enforcement observed the sedan to be a dark-colored Chevy Spark with Maryland tag 4DD1082. At approximately 10:44 p.m., a GPS ping within an uncertainty range of approximately twenty-one meters in diameter showed that TT1 was on I-40 eastbound near Raleigh, North Carolina.

27. Law enforcement followed the Chevy Spark from around Cary, North Carolina, to near Rocky Mount, North Carolina, at which point the Chevy Spark traveled north on Interstate 95. Subsequent GPS pings showed TT1 travel from North Carolina back north and arriving at BARRERA ALACHAN's house in Catonsville, Maryland, at approximately 4:00 a.m. on or about March 17, 2018. At approximately 9:25 a.m. the same day, law enforcement surveillance observed the same dark-colored Chevy Spark with Maryland tag 4DD1082 parked in the vicinity of 318 Melvin Avenue in Catonsville. A GPS ping at approximately 9:23 a.m. showed that TT1 was in the vicinity of 318 Melvin Avenue, Catonsville, within an uncertainty range of approximately sixteen meters.

28. Later that day, at approximately 11:16 a.m., UC-1 communicated with BARRERA ALACHAN via TT1 to arrange a deal to sell UC-1 three ounces of cocaine. Most of the calls were recorded. BARRERA ALACHAN agreed to meet UC-1 in an undercover vehicle in the same meeting spot in Prince William County that day. When UC-1 arrived, UC-1 called BARRERA ALACHAN and asked "are you still in your car?" BARRERA ALACHAN said "yes, I am in a black car." BARRERA ALACHAN was observed by law enforcement driving the same dark-

colored Chevy Spark with Maryland tag 4DD1082. At the meeting, UC-1 and UC-2 gave BARRERA ALACHAN $2,700 of controlled funds and received three ounces of suspected cocaine. The substance later field-tested positive for the presence of cocaine.

29. As noted above, SALGADO was identified as the user of TT2, and as being associated with the **Target Location**. Specifically, an open source search of the address associated with the **Target Location** revealed that SALGADO set up a utility at this address in 2016. A query of law enforcement databases showed that SALGADO had been previously arrested in California and in Reno, Nevada; investigators obtained the booking photograph from SALGADO's 2006 arrest in Nevada.

30. Thereafter, on or about March 31, 2018, law enforcement surveilling BARRERA ALACHAN tracked him to a Shell gas station at 3916 Goldsboro Road in Wade, North Carolina. Thereafter, two other Hispanic males arrived at the gas station; one of them was driving the **Target Vehicle**, which was towing a trailer. Law enforcement observed a wheel on the right side of the trailer fall off. Video and photographic evidence of the incident was obtained, including the following:

31. Based on a comparison of the 2006 arrest photograph of SALGADO, and the photographs and video from the March 31 surveillance, law enforcement determined that SALGADO is the male wearing the white hat and kneeling down in the picture above, who had been driving the **Target Vehicle** and towing the trailer. BARRERA ALACHAN is wearing the black leather jacket.

a. Law enforcement later determined that SALGADO is the user of TT2 because during the period of interception of TT2, SALGADO received a phone call from an unidentified male caller using the phone number (910) 386-2248 who asked him, "How are we, Homero?" to which SALGADO responded, "Here."

b. Additionally, on or about July 16, 2018, SALGADO placed an outgoing call on TT2 to the Mexican phone number +52 176 7120 0633. During the call, the unidentified male caller asked SALGADO how "they" were doing and then asked, "Are you Homero?";

SALGADO responded, "Yes." The unidentified male then asked again, "You are Homero, right?"; SALGADO again responded, "Yes." The unidentified male then asked a third time, "Are you Homero?"; and SALGADO responded a third time, "Yes."

32. On or about May 24, 2018, at approximately 8:59 p.m., UC-1 coordinated with BARRERA ALACHAN, using TT1, to purchase approximately four ounces of cocaine. The next day, at approximately 8:26 a.m., law enforcement lawfully intercepted and translated a call between BARRERA ALACHAN, using TT1, and SALGADO, using TT2. BARRERA ALACHAN said, "I think they are going to be like 8 or 9." SALGADO assented. BARRERA ALACHAN explained, "Since I only had enough right now for four little tires so I'm going to bring you those and I'm going to take them and then I'm going to go get the other five." Later in the conversation, BARRERA ALACHAN told SALGADO that he would call him when he was at exit 79 so they could determine where to meet. At approximately 3:19 p.m., BARRERA ALACHAN called SALGADO and asked, "where do you want me to meet you? Do you want to meet somewhere around there, or you want me to go all the way there?" SALGADO responded, "Eh, that you come here, cousin." At approximately 10:19 p.m., BARRERA ALACHAN called SALGADO and said, "Here, I will be there in six minutes." SALGADO responded, "That's fine cousin, I am about to get home right now." GPS data from May 25, 2018, shows that TT1 was in the vicinity of the **Target Location** from approximately 10:35 to 10:40 p.m. The GPS pings were accurate within an uncertainty range of eight to sixteen meters.

33. On or about May 26, 2018 at approximately 8:25 a.m., law enforcement lawfully intercepted and translated a call between BARRERA ALACHAN, using TT1, and SALGADO,

using TT2. During the call, BARRERA ALACHAN told SALGADO that he (BARRERA ALACHAN) would arrive around 1:30 or 2:00 p.m. SALGADO responded, "It is better over here. At 1:30 p.m. it is better here, where I work. I don't like going over there too much, you going around that area much. To tell you the truth, we cannot do that. It is better here where we work; it is quieter." Based on the context of the conversation, I believe that SALGADO was telling BARRERA ALACHAN not to meet at his house (the **Target Location**) again, but rather to meet at an area near SALGADO's work. BARRERA ALACHAN then said he would call SALGADO when he was close to "Exit 79," half an hour before. SALGADO instructed BARRERA ALACHAN to meet at the usual place. BARRERA ALACHAN asked, "Where we stayed at that time?" SALGADO then said, "Where my trailer broke off?," and BARRERA ALACHAN confirmed. BARRERA ALACHAN then advised that he would call when he was close to the meeting location.

34. Later on May 26, 2018, GPS location data on TT1 showed that BARRERA ALACHAN traveled from Maryland to North Carolina. BARRERA ALACHAN continued to communicate with SALGADO until he reached the meeting location, at which time law enforcement conducting surveillance observed BARRERA ALACHAN meet with SALGADO (who was not driving the **Target Vehicle**) at the gas pumps of the same Shell station at 3916 Goldsboro Road in Wade, North Carolina, where law enforcement had observed the wheel of SALGADO's trailer fall off on or about March 31, 2018. GPS location data on TT1 over this period of time confirmed that it was in the area of the Shell gas station, within an uncertainty range of eight meters to 134 meters. Surveillance observed the meeting until BARRERA ALACHAN

left the area at approximately 2:57 p.m.

35. Thereafter, GPS location data and law enforcement surveillance established that BARRERA ALACHAN traveled back to northern Virginia and met with UC-1 and UC-2 at a parking lot in Prince William County, Virginia, at approximately 7:41 p.m. In this transaction, which was audio and video recorded, UC-1 exchanged $3,600 in controlled funds for approximately four ounces of suspected cocaine. The substance field-tested positive for the presence of cocaine. I believe that the call referenced in paragraph 33 was to arrange the meeting that is described in paragraph 34. Based on my training and experience, I believe that during the meeting in paragraph 34, BARRERA ALACHAN acquired the powder cocaine from SALGADO for resale to UC-1 and UC-2. During the transaction, UC-1 asked BARRERA ALACHAN about purchasing crystal methamphetamine. BARRERA ALACHAN advised that he had a contact that could get it and would ask his contact about it.

36. Later that evening, at approximately 10:12 p.m., law enforcement lawfully intercepted and translated a call between SALGADO, using TT2, and BARRERA ALACHAN, using TT1. BARRERA ALACHAN advised SALGADO that he left the job in Virginia and that he would return to SALGADO's location next Saturday. BARRERA ALACHAN said that "he" (an unidentified third person, believed to be UC-1) asked BARRERA ALACHAN if SALGADO could get "crystal" and what the price would be. SALGADO told BARRERA ALACHAN that he would inquire and let BARRERA ALACHAN know. I believe, based on my training, knowledge, and experience, that BARRERA ALACHAN and SALGADO were using coded language to discuss the sale of methamphetamine for UC-1.

37. On or about June 9, 2018, law enforcement observed BARRERA ALACHAN arrive to an AutoZone store in Fayetteville, North Carolina. At approximately 10:25 a.m., SALGADO left his place of employment in the **Target Vehicle** and drove to the AutoZone, where he parked next to BARRERA ALACHAN. The two men met briefly between their vehicles, and then moved to the front of their vehicles. Then, at approximately 10:55 a.m., BARRERA ALACHAN and SALGADO left the AutoZone; SALGADO drove the **Target Vehicle** back to his place of employment.

38. On or about Thursday, August 2, 2018, at approximately 8:54 p.m., SALGADO (on TT2), called BARRERA ALACHAN (on TT1). During the conversation, BARRERA ALACHAN said, "I'm going to stop by over there on Saturday." SALGADO answers, "Ah, okay, you said it." BARRERA ALACHAN said, "A number four [4], there." Salgado responded, "That's fine, cousin." BARRERA ALACHAN continued, "Yes because if another little tire comes up I will call you." SALGADO replied, "That's fine -- that's fine, of course." BARRERA ALACHAN then said, "Yes, I'm going to be there early, we are leaving from here around two [2]." SALGADO asked, "Ah okay, around what time are going to be there?" BARRERA ALACHAN responded, "I think 8:30." SALGADO said, "8:30 that way I get there at that time, that ways I leave from here to be there at 8:30 so that way I don't arrive there with the tires over there, to the -- the shop." BARRERA ALACHAN stated, "I'm going to call you when around 69 from there." SALGADO said, "That way I also head over there." Salgado continued, "Let me know if anything, if the numbers change." BARRERA ALACHAN stated, "Yeah, I will call you but regardless, I will call you tomorrow." SALGADO replied, "That's fine cousin, of course."

39. Based on my training, experience, and knowledge of this case, I believe that SALGADO called BARRERA ALACHAN to confirm the purchase of narcotics on the following Saturday, which was August 4. Furthermore, I believe that SALGADO and BARRERA ALACHAN were using code for narcotics when they used the term "tires." Furthermore, I believe that when SALGADO stated, "8:30 that way I get there at that time, that ways I leave from here to be there at 8:30 so that way I don't arrive there with the tires over there, to the -- the shop," he was telling BARRERA ALACHAN that he would travel directly from the **Target Location** (*i.e.*, his residence) to meet with BARRERA ALACHAN so that he would not have to bring the specified cocaine to into his place of business. GPS location data on TT1 showed that on or about August 4, 2018, at approximately 7:58 a.m., TT1 was in the vicinity of a gas station near SALGADO's place of employment, within an uncertainty range of twelve meters. Approximately thirteen minutes later, at 8:11 a.m., a pole camera placed outside of SALGADO's place of employment captured him arriving at the business in the **Target Vehicle**. At approximately 8:15 a.m., TT1 was already on its way back to Maryland.

40. On or about August 16, 2018, law enforcement officers established surveillance in the early morning hours in the vicinity of the **Target Location**. Surveillance observed the **Target Vehicle** parked near the front of the trailer at the **Target Location**. Approximately two hours later, surveillance observed the **Target Vehicle** at an intersection near the **Target Location**. The **Target Vehicle** was driving in the direction of SALGADO's known place of employment in Fayetteville. Surveillance confirmed, based on earlier surveillance and a comparison with a photograph from a prior arrest, that the driver was SALGADO. Surveillance also confirmed that

the **Target Vehicle** had North Carolina license plate number HT 2695.

41. On or about September 21, 2018, GPS location data for TT1 showed that the phone traveled from Maryland to North Carolina. A review of toll records for the next day — on or about September 22 — showed that at approximately 12:50 a.m., BARRERA ALACHAN called SALGADO and spoke for approximately ninety seconds. Then, at approximately 1:15 a.m., TT1 pinged for approximately thirty minutes at the **Target Location**, which is SALGADO's known residence. The uncertainty range for the time TT1 was at that location was between five and fourteen meters. Furthermore, SALGADO's phone (TT2) pinged at that same location during the same time with an uncertainty range of seven to fifteen meters. After leaving the **Target Location**, BARRERA ALACHAN spent the night in a neighboring town before traveling back to Maryland. When he returned to Maryland, he was observed arriving at home with a female passenger. Both the female passenger and BARRERA ALACHAN were observed holding bags as they entered BARRERA ALACHAN's residence. Based on my training, experience, and knowledge of this case, I believe that BARRERA ALACHAN traveled to meet SALGADO at the **Target Location** to obtain distribution quantities of narcotics to be redistributed in the greater Washington DC area.

42. On or about October 12, 2018, law enforcement drove past the **Target Location** at approximately 11:21 p.m. Officers observed the **Target Vehicle** parked in front of the **Target Location**.

43. Based on the pattern of activity explained throughout this affidavit, I believe SALGADO facilitates and engages in the sale and distribution of illegal drugs, including from his residence at the **Target Location**, and through the use of the Target Vehicle. There is thus

probable cause to believe that evidence of a conspiracy to distribute controlled substances in violation of 21 United States Code, Sections 841(a)(1) and 846, and evidence of the use of a communication facility to commit controlled substances offenses, in violation of 21 United States Code, Section 843(b), will be found at the Target Location and in the Target Vehicle.

ELECTRONIC EVIDENCE

44. Pursuant to Rule 41(e)(2)(B), the warrant applied for would also authorize the seizure or, potentially, the copying, of electronically stored information within any seized digital devices and electronic storage media. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

45. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found in the Target Locations or Target Vehicle, there is probable cause to believe that the records and

information described in Attachment B will be stored in such media or devices for, but not limited to, the following reasons:

a. Individuals who engage in criminal activities, including the distribution of controlled substances and/or illicit firearms, use digital devices to communicate with co-conspirators online, but they also store on computer hard drives and other electronic storage media records relating to their illegal activity. Online criminals store these documents and records, which can include logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things:

i. keep track of co-conspirators' contact information;

ii. keep a record of illegal transactions for future reference;

iii. keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and

iv. store stolen data for future exploitation.

b. Such individuals, in the event they change devices, will often "back up" or transfer files from their old devices to their new devices so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their

criminal activity.

c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media — in particular, computers' internal hard drives — contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this

evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

46. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the seized items were used, the purpose of their use, who used them, and when. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. There is probable cause to believe that this forensic electronic evidence will be on any digital device or storage medium found in the Target Locations or the Target Vehicle because:

47. Data on the device or storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were

recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

48. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

49. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

50. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

51. I know that when an individual uses a digital device to engage in criminal activities,

including criminal conspiracies, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

52. *Methods to search digital devices*. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who

have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious

software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not able to be segregated from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition,

digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such

mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying digital devices and/or storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose may parts of a hard drive to human inspection in order to determine whether it is or contains evidence described by the warrant.

CONCLUSION

WHEREFORE, I respectfully request the issuance of this Search Warrant based on the facts contained within this Affidavit, which support probable cause to search the premises located at 903 Frank Wicker Road, Sanford, North Carolina (the **Target Location**) and a gray Dodge Ram pick-up truck bearing North Carolina plate HT 2695, VIN 1D7HU18D74J265329 (the **Target Vehicle**), as further described in Attachment C, for evidence related to violations of Title 21, United States Code, Sections 841(a)(1), 843(b), and 846, as further described in Attachment B.

Stephen Razik
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me this 22nd day of October, 2018.

L. PATRICK AULD
United States Magistrate Judge
Middle District of North Carolina